STRATEGIC MILITARY COMMUNICATIONS OF THE FUTURE: LEVERAGING CIVILIAN OPERATIONS

BY

CAPTAIN PHILIP S. PRITULSKY
United States Navy

USAWC CLASS OF 1998

USAWC STRATEGY RESEARCH PROJECT

Strategic Military Communications of the Future: Leveraging Civilian Operations

by

Captain Philip S. Pritulsky

Professor Robert Minehart
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Captain Philip S. Pritulsky

TITLE: Strategic Military Communications of the Future: Leveraging Civilian Operations

FORMAT: Strategy Research Project

DATE: 14 March 1998 PAGES: 52 CLASSIFICATION: Unclassified

The Department of Defense is transiting from a technology driver to a technology rider in strategic communications. Today 95% of all military communications travel a portion of their routing via commercial public switched networks. Early in the 21st century, a new generation of commercial systems will serve as the backbone for all military communications.

This extensive leveraging of civilian technology provides tremendous efficiencies for the government. However, with the emergence of the threat of Information Warfare (IW), we must assess the strategic implications of America's reliance on civilian information infrastructures? Does this reliance pose an unacceptable risk to national security?

This paper examines the broad implications of military leveraging of strategic communications. It uses the Strategic Principles of War for the 21st Century to assess the impact of this policy on military preparedness.

TABLE OF CONTENTS

LIST OF TABLES

As the Information Age accelerates the world into the 21st century, various commercial ventures are weaving its web of communication infrastructures into a global information grid. This "Globalization"[1] of telecommunications is shaping a new era in human culture, a culture which increasingly values being connected.[2]

The U.S. military is also being shaped by this explosion of information and connectivity and at a critical point in its history. America's armed forces are currently in transition. Declining fiscal resources are forcing the U.S. Department of Defense (DoD) to "build down"[3] its forces and carry out its mission with a smaller budget. In the future, all military strategic communications will reside in the world's information grids. Military users will shift to an unfamiliar role as dependent customers of these systems. This will signal the end of an epic era of U.S. military supremacy, as the peerless owners of space based communications.

However, leveraging these tremendous advancements in civilian operations for military uses is an uncomfortable concept

within a broad context of the military. Military strategists fear a loss of control and the possible compromise of security. Although such implications about leveraging may be unwarranted, military leaders must now think in different terms, both about their strategic objectives and future organizations. This paper examines these implications for future military communications using the Strategic Principles of Warfare for the 21st Century.[4]

BACKGROUND

Principles of War

	Strategic		Traditional
1.	Objective	-	Objective
2.	Initiative	-	Offensive
3.	Unity of Effort	-	Unity of Command
4.	Focus	-	Mass
5.	Economy of Effort	-	Economy of Force
6.	Orchestration	-	Maneuver
7.	Clarity	-	Simplicity
8.	Surprise	-	Surprise
9.	Security	-	Security

Table 1.

The traditional Principles of War (Table 1) are the enduring bedrock of military doctrine.[5] Viewed as universally applicable, they offer guidance to operational commanders about the conduct

of warfare. However, at the strategic level many theorists contend all Principles of War can be distilled down to only two:

1. Take all possible actions to increase your own effectiveness and efficiency.
2. Take all possible actions to erode your opponent's effectiveness and efficiency.[6]

The Army's Strategic Studies Institute developed the "Strategic Principles of War for the 21st Century" to provide current military strategists with a framework to examine strategic policies more systematically and with greater granularity. Policy implications, such as leveraging civilian operations, can now be viewed from the perspective of future operational commanders.[7]

DoD's future objective is "Information Superiority." Leveraging strategic communications is now its central policy to achieve this objective. However, practical evaluation of this strategy must come from a warfighter's analysis of its planned implementation.

The Strategic Principles of War provide such a metric. They focus on ways to achieve a desired endstate, such as Information Superiority, by leveraging civilian strategic communications.

In the application of these Strategic Principles of War which follows, each Strategic Principle of War is defined, and its traditional Principle of War is noted in parentheses.

ANALYSIS

1. *Objective:* *(Objective) Identify and pursue a clearly defined and attainable goal whose achievement best furthers the national interests(s).*[8]

Protect the nation's fundamental and enduring needs; the lives and safety of its people; maintain American sovereignty with its values, institutions and territory intact; and provide for the prosperity of the nation and its people.[9] This National Security Strategy objective for defending America is exceedingly clear.

Although strategic communications are a critical element in America's defense, the history of strategic communications reveals a constant theme of change. Further, this change has accelerated exponentially in recent few decades.

Development of nuclear-tipped Intercontinental Ballistic Missiles (ICBM's) prompted even faster methods of strategic communications. Space-based command and control systems eventually responded to this nuclear-age urgency. Today, information dispersion, system ownership and the military's role in the communication arena are in transformation. The Defense Information System Agency's (DISA) Master Plan reflects DoD's shift in policy initiatives to create this information based environment for communication and information exchange.[10]

Since earliest times, strategic communications have facilitated the exchange of information essential for conducting the affairs of nation states, including the conduct of war. The strength of these communications was in their ability to rapidly transfer information from the source to intended recipients, by means of a protected, survivable, and secure means, without compromise or loss of message integrity.

"Information Superiority" relies on these same fundamental imperatives. In "Joint Vision 2010," the Chairman, Joint Chiefs of Staff, specifically identifies "Information Superiority" as the primary enabler of military forces in future warfare.[11]

Since strategic communications will be a subset of these global information grids, Information Superiority will ultimately involve the control and mastery of these grids. Thus U.S. military's robust commitment to leveraging civilian systems which form these grids is primarily a commitment to its own ultimate objective of Information Superiority.

Current military strategic communications rely on the DoD's Satellite Communications (SATCOM) system. In the future, a commercial SATCOM architecture will provide the foundation for global information grids and thus the backbone of U.S. strategic communication. DoD envisions its own future architecture within this context, specifying its need for mobile, high capacity, protected (anti-jam), survivable, and secure communications for its military users.[12]

However, DoD is also facing the necessity to develop a new architectural solution for its current military SATCOM systems which will all reach their terminal lifespans by Fiscal Year-2017 and require replacement.[13]

Although satellite replacement is ostensibly driving this change of policy, it also corresponds with DoD's long term objective for Information Superiority. Cost and technical enhancements, especially in view of the phenomenal pace of change, will not permit the military to achieve this goal unaided. The technological lifespan of satellite communication systems has shrunk to less than the government's current acquisition timeline to develop, acquire, and deploy its own new systems. Meanwhile, industry's development and deployment cycle is much faster and more responsive.

The significant difference between government and industry is evident in their continuing exploitation of space: the National Security and civilian space expenditures are approaching parity. Significant recent growth in overall space systems is due primarily to the increases in the civil space sector. While the National Security space budget remains fairly static at about $14 billion for 1998, the Department of Commerce estimates all commercial space activity in 1998 to be about $8 billion, a number which is expected to double in the next ten years.[14] Undoubtedly, the future of space will rest in the commercial sector.

Likewise, the military must recognize that in historical perspective the relationship between invention and the military has been steeped in leveraging. Modern military warriors need only to look back beyond the past two hundred years to realize the tools of war were not always wholly different from the tools of life. Although some current military leaders lament that technical and fiscal decisions are undermining military control and ownership, the real objective remains clear: Defend America! If civilian systems satisfy this need with acceptable risk, then the means portion of the National Security Strategy equation is being met.

2. *Initiative (Offensive): Seize, retain and exploit the initiative.*[15]

About the Future:

"Never have so many understood so little about so much"[16]

– James Burke "Connections"

America must seize the strategic initiative today if it desires to ensure Information Superiority in the future. But such initiative poses a critical question: Can the U.S.

accurately predict the future capabilities it will require, as well as those of its enemies?

Designating space as a new geographical area for National Military Commanders has added a new dimension of thinking about the battlefield. Information warfare provokes similar new thinking. Like space, information infrastructures are only a medium that creates battlefields in a new virtual world. However, unlike space, the information infrastructure medium itself can also be the target of attacks.

As on any battlefield, initiative in strategic communications must first provide future military commanders with freedom of movement throughout these global grids. The military must therefore have a strategy which aggressively seeks a footprint in each new technology. An incidental benefit of acquiring this tremendous access will be widespread system redundancy. Information Superiority however, will require more than simply having access to the battlefield. Warfighters must also have the necessary offensive and defensive weapons to exploit the informational battlefield to achieve superiority. Access, in and of itself, does not guarantee mastery.

The military must therefore expand its concept of communication, including strategic communications, from the traditional paradigm of providers and users, to that of a dynamic environment in which to conduct offensive and defensive operations. A modern military force must have the capability to apply its nation's strategic informational firepower within and throughout global information grids.

Future forces will require not only tools but also technical understanding of global networks, down to an actual user system level. They will require trained people with knowledge of the Common Operating Environment (COE) which an adversary employs within his various systems, as well as knowledge of the types of applications working in this environment.[17] These "information soldiers" will need the support of national intelligence assets dedicated to "data-mining," which will "take advantage of vast amounts of data being collected and stored in various, often unrelated databases" within an adversary's systems[18].

America's military must develop its own force of professional Information Operations (IO) warriors. Certainly the cadre of geographical, warfighting CINC's will vigorously fight

for control of such a force. However, in a virtual world, the physical location of any offensive force is inconsequential. Rather, the measure of offensive effectiveness will be the accurate and rapid application of force against a target. Likewise, such attacks will also demand appropriate prior coordination and a thorough understanding of the anticipated second and third order effects. The National Defense Panel has recommended creation of a U.S. Forces Command, located in the United States with the capacity to conduct Information Operations support to the warfighters anywhere around the globe.[19]

Finally, initiative must also consider denying the ways and means of preventing future adversaries' access to these grids. The first two decades of the twenty-first century will see the global information grid fully established and refined.[20] It will create a system of redundant wireless networks relying on multiple, low and medium earth orbiting satellites (LEO/MEO), terrestrial microwave and fiber optic backbone systems.[21] Western nations have already begun to field these global strategic communication capabilities. Any attempts to slow diffusion of technology to other civilizations or potential

future enemies will be increasingly difficult, if not impossible to stop.[22]

3. *Unity of Effort (Unity of Command): For every objective coordinate all activities to achieve unity of effort.*[23]

Global Partnerships and "Condottiere" Fighters

Future unity of effort will necessitate non-military partners to work closely in concert with DoD. These partners will include other elements of government, commercial, law enforcement and even international governments and corporations. Dr. Paul Kaminski, the Under Secretary of Defense for Acquisition and Technology cites four sectors competing for space infrastructures: Civil, Commercial, International and National Security. He cautions that "managing for tomorrow will require thinking 'out-of-the-box' to develop and implement a vision for the future."[24]

Such out of the box thinking has already led the U.S. military to become the first major customer to purchase a high

capacity gateway connection to Motorola's new worldwide, wireless communication system IRIDIUM.[25] Interestingly, financing IRIDIUM is a network of eighteen global investment partners covering every country in the world which will receive service.[26]

U.S. Ownership of an IRIDIUM network control center now provides America with a primary means to access this new technology.[27] Undoubtedly, U.S. entry into any technology, whether as a new partner or simply as a customer, will trigger similar demands for access by other governments wary of American domination of such technology. Likewise, as all communications become fully resident in the information grids, there will be no precise dividing lines between strategic, operational, or tactical communications. Nor will the roles of the military, police, government, or industry be precisely or unequivocally defined in the future.

Governments must therefore critically evaluate their security concerns in any such transnational partnerships. Any governmental influence on such companies will have tremendous political, economic and security implications to all other users. Likewise, foreign government ownership of companies dealing in

strategic telecommunications presents significant risks. Although U.S. law prohibits its military from purchasing or operating companies, law enforcement and intelligence agencies have fewer restrictions in fronting such operations. Undoubtedly, each new partnership will complicate the unity of effort and raise the level of risk among multinational users.

Governments must also recognize the primary concern of businesses is their bottom line profit. Undoubtedly, larger customers will merit special advantages. Unfortunately, DoD's shrinking budget no longer earns it the same level of influence in the marketplace it once enjoyed. Therefore, DoD must innovatively target its research and development spending to enhance areas most beneficial to its objectives for future success.

To this end, the U.S. Space Command is pioneering a new concept entitled "Global Partnerships." This program seeks to strengthen DoD space capabilities and enhance confidence in coalition warfare by leveraging domestic, national, international, military, civil, and commercial resources.

The "Full Force Integration" plan under consideration by U.S. Space Command identifies several areas for high partnership potential. These prospective partnerships represent a fundamental shift in U.S. thinking about achieving space warfighting capabilities. Still in the embryonic stages of development, the Space Command's success will hinge on the availability of resources, corporate profit expectations, and the divergent interests of corporations and allies.[28]

These global partnerships seem to increase security for both the U.S. and its international allies. Such partnerships could expand a protective U.S. umbrella to other nations for worldwide missile defense, information assurance, and global surveillance and warning. Such partnerships will be demanding, both in the efforts to achieve and to maintain them. However, the promised offset in benefits could result in a reduction of threats and increased cooperation.

This emerging reliance on commercial infrastructures appears to place governments in a secondary role to the interests of economic entities. It also invokes Macheivilli's caution to the Italian nation states of the 15th century: their protection

depended upon the allegiance of contracted warfighters, "Condottiere", paid to provide for their national defense. For totally reliable strategic communications, the U.S. government and its military will need unqualified unity of effort in their partnerships with industry. Without new, innovative ways to achieve this prospect the commercial communication and satellite corporations will not be far removed from the "Condottiere" fighters of the past. Macheivilli's warning will not be without merit.[29]

4. *Focus (Mass): Concentrate the elements of national power at the place and time which best furthers pursuit of the primary national objective.*[30]

Eliminating the Seams:

For the U.S. is to possess a future ability to concentrate its elements of power, it must eliminate the seams between the various military services, governmental agencies and departments, and corporate partners. These seams may be procedural, organizational, or jurisdictional. Regardless of their source, they exacerbate the differences and create friction in the communication process. In the accelerated pace of information

warfare, delays, distrust, lack of clear jurisdictional boundaries and friction will enhance an adversary's advantages and maneuvering space in a virtual battlespace. A "national level of trust" must be instituted which transcends the current organizational impediments to these various entities.

Eliminating friction and creating a national trust will demand new processes, security procedures, and even a new concept of organizations. Massing these various elements, although difficult, will be essential for an effective defense against attacks to America's information infrastructures. Ultimately even the government's decision-making process will need reform. Organizations at every level, from the National Security Council (NSC) to field commanders will have to accelerate their decision making in the future.

For the U.S. the critical issue is to develop the means to differentiate between warfare, mischief, or criminal activity directed at its strategic communication networks. The President's Commission on Critical Infrastructure Protection identified several proposals to accomplish these objectives.[31] A national level Indications and Warning capability must first

provide immediate, real-time detection of an attempted cyber attack on critical infrastructures. Additionally, the Commission called for creation of an Information Operational Analysis Center (IOAC). This facility would act as a clearing house to monitor America's infrastructures and keep the appropriate government and private sector users informed.[32] Ultimately, the crucial underpinning for any increased coordination will depend on new levels of national trust among all parties focusing on this problem.

5. *Economy of Effort (Economy of Force): Allocate minimum essential resources to subordinate priorities.*[33]

Redundancy and the Defense Technology and Industrial Base (DTIB):

Economy of effort has three major components: the resources available, their effectiveness, and their efficiency. The down side risk of too much economy of effort is that the perception of national power resides in a combination of actual and potential strengths and weaknesses.[34] Thus the merit of Information Superiority will rest on the United States' resolve to execute

its national will, coupled with its actual ability to attack, defend, and restore its strategic communications infrastructure.

Economy of force seeks to avoid wasting resources. However, the government must not economize budgets by investing only in leveraging strategic communications. It must also support investment in commercial research and development for infrastructure repair and reconstitution and demonstrate resolve to recover from an information attack. Likewise, it must encourage developing redundancies for commercial systems in other areas of the electronic spectrum. Advances in High Frequency bandwidths potentially offer new alternatives to space systems, should they fail.

Certainly large-scale reductions in defense research, development, and procurement threaten the Defense Technology and Industrial Base. Current projections predict the DTIB will be inadequate to maintain U.S. superpower status in the future.[35]

In strategic communications, a new theory of Commercial-Military Integration (CMI) offers promise for both the military and industry. The goal of CMI is to identify common production

elements and processes which satisfy both the needs of industry and defense. This concept of "Dual-Use Technology and Production," advocated by President Clinton, will allow the armed forces to exploit the rapid rate of innovation and market driven efficiencies of commercial industry to meet defense needs.[36] In the future, Economy of Force will demand DoD blend the DTIB with civilian industries in creative ways to ensure national security.

6. *Orchestration (Maneuver): Orchestrate the application of resources at the times, places, and in ways which best further the accomplishment of the objective.*[37]

Standardization

Future military operations will require a much higher degree of orchestration than in the past. This orchestration will rely on development of International Alliances, Global Partnerships, Commercial-Military Integration, and national level trust. This will indeed be an immensely complicated process.

Yet the measure of successful orchestration in communication, will be determined neither by the speed nor by the throughput of transmitting information. Rather the measure will

be the timeliness of decision making and ease of accomplishing it.

Governments will continue to have a role in this orchestration through the process of standardization. Industry and the marketplace themselves have the ability to establish standards for software, hardware, and communication compatibility. However, they may not be able to standardize as effectively without agreements from the various forums of nation states which already deal with such issues.

Standardization agreements will ensure global access and efficiency of communications. Orchestration will thus rely, not on the leveraging of civilian operations for strategic communications but on how quickly the various governmental and military organizations change to adapt and deal with these increased communication capabilities.

7. *Clarity (Simplicity): Prepare clear strategies that do not exceed the abilities of the organizations that will implement them.*[38]

Changing Roles:

Clarity will remain the most difficult of the principles to achieve and articulate. Leveraging civilian operations for strategic military communications seems forthright enough as a policy statement. Strategically, leveraging has implications far beyond the military organizations which must execute operations in cyberworld.

Americans are fiercely protective of their constitutional rights. Terms like information superiority, dominance, assurance and complete battlefield knowledge confer a high-tech sense of well being. They also make people uneasy and skeptical. Those who value their privacy increasingly fear the government, through their armed forces, might be invading their workplaces, libraries, or homes.

Americans are comfortable with strong constitutional constraints on their military. New roles, such as defending America's national infrastructure, could place the military into areas where it is not specifically comfortable. Although the military may view such roles as essential for national security, some citizens may not agree. Americans prefer a clear distinction between the police and the military. Any blurring of

these roles may eventually result in shifting more responsibility to law enforcement to ensure protection of her citizens' liberties.

Thus any transformation to new roles for America's military forces will require preparing both the military and the American public. Successful future information operations will depend on the government's and the military's ability to clearly develop and articulate these new roles.

Military and government leaders must also clearly define the new battlefield of cyberworld, state its strategic importance and then build the appropriate organizations to carry out the National Security Strategy mandate. This means justifying the need to leverage civilian systems and create partnerships with law enforcement, industry, and allies to support its strategic objective. If U.S. leaders can successfully articulate these concepts, they can gain support from their own citizens, corporations and allies to achieve this objective.

Changes must first start with the military's traditional concept of its dual roles in communication - the warfighter's

need to communicate coupled with the combat support perspective on how to make it happen. The military takes great pride in its developmental role in space systems. However, the future of space-based communications will belong to commercial interests. The military will have to reform its long held concept of space and strategic communications and embrace a new reality of sharing with others.

The military thus faces several dilemmas. To fully leverage new information grids, it must first relinquish its own systems. Concurrently, it must also create offensive and defensive specialists who fully understand civilian information grids in order to conduct warfare. Having lost ownership of these systems it will be more difficult to develop military specialists without placing greater reliance on civilian ones. Recognizing these multiple dilemmas accounts for the military's caution in fully embracing these new telecommunication architectures.

8. *Surprise: (Surprise) Accrue disproportionate advantage through action for which an adversary is not prepared.*[39]

Decision Cycles and Treaties:

Information is becoming a commodity in which commercial industries have strongly held interests. As a country with much to lose in an Information War, U.S. policy makers must consider mobilizing world alliances to eliminate information grids as a potential battlefield.

To achieve surprise in the future, just as today, will involve coordinating many disparate activities. Surprise could be very effective, if America has the means to work inside an enemy's decision-making cycle to preempt or prevent its actions. Conversely, information grids inherently provide great protection and anonymity to all users. For America to prevent surprises against itself, it must develop new computer aids for quickly tracing information actions back to their source. Information Superiority must support both offensive and defensive capabilities.

Surprise will still involve the traditional element of remaining undetected. However, information grids will make achieving it more complicated. More actors other than one's enemies will be seeking to preempt America's surprise. These will include other nations, world news services and intelligence

gathering corporations. All of these elements combine to decrease the U.S.' ability to limit or control dissemination of information, thus weakening the effectiveness of surprise.

Possible disruptions attributed to Information Warfare may actually create a backlash of world opinion against this new form of warfare. John Arquilla recently postulated a "Great Global Cyberwar" where the enemy was invisible, the battles virtual, and the casualties real.[40] His article also hypothesized such a war would initiate a global movement towards international treaties banning the use of the information grids for war.

The Cold War led to creation of nuclear policies such as Mutual Assured Destruction (MAD) and eventually to the universal recognition that nuclear warfare was unacceptable at any level of war. If Mr. Arquilla's projections hold true, Information Warfare will undoubtedly face similar consequences. Because of the potential lethality and destructiveness of Information Warfare attacks, nation states will be reluctant to use them if they might face unfavorable world opinion.

Thus treaties banning warfare on the information grids are not an unrealistic prospect. International treaties restricting military operations in Antarctica and Space already exist. In strategic communications, the International Maritime Satellite Organization (INMARSAT) consortium (comprised of 72 member nations) agreed in 1979 that "the organization shall act exclusively for peaceful purposes."[41] There is general agreement that this means the use of INMARSAT must be "unrelated to armed conflict."[42] The DoD relegates its use of INMARSAT communication only for purposes of administrative, non-aggressive support of combatant forces. Multinational consortiums involved with information grids could advocate for similar agreements. Treaties however, will not hamper criminals, terrorists or non-signers. And although they will restrict nation states and military efforts, world opinion may demand their implementation.

Achieving surprise in the future will be even more difficult. American decision-makers must therefore streamline organizations and processes to permit actions which help to develop surprise and prepare the United States for this future.

9. *Security: (Security) Minimize the vulnerability of strategic plans, activities, relationships, and systems to manipulation and interference by opponents.*[43]

The Threat:

America may now face greater threats to her own internal security than at any time in her history. While traditional military warfighting roles remain fundamental, their force structure, tactics and capabilities will change significantly. Information Superiority will be the new key enabler to protecting these forces in an information environment, and cryptologic systems will be the key to Information Superiority. Cryptology provides critical protection and security of information, whether it travels via military or civilian communication systems. Yet crytologic technology is rapidly evolving and proliferating. Like any core competency, cryptology is vulnerable, perishable, and exploitable.

Information Warfare offers the promise of low cost, long-distance striking ability, offering potentially high payoffs and small risk of detection or identification. IW will be an attractive tool for asymmetrical warfare. Likewise, pressures to

exploit, steal, or deny America of its vital cryptologic capabilities will expand accordingly. Threats will come not only from external nation-states but from a variety of sources - including criminals, terrorists, and even corporate aggressors, both national and international, who desire access to America's information systems. In its report on Information Warfare-Defense the Defense Science Board Task Board noted, "Increased reliance on information systems...creates a tunnel of vulnerability previously unrealized in the history of conflict."[44] Defending America's information systems and infrastructures could well be the next battleground for its forces.

As all these potential threats to U.S. vital interests are expanding, some strategists question whether U.S. and Western dominance over the last two hundred years is actually diminishing. They believe that countries, like the U.S., are reaching parity with other world nations due to the enormous rate of technology transfer they provide. Their view of globalization of technology is a sign that Western societies are in decline.

Clarance Huntingdon contends that by the middle of the 21st century the two hundred year Western "blip" of dominance over the world's economies will end.[45] Huntingdon anticipates that by 2020 Western nations will most likely only control about 24 percent of the world's territory (down from 49 percent), 10 percent of the total world population (down from 48 percent), about 30 percent of the world's economic product (down from a peak of probably about 70 percent), perhaps 25 percent of manufacturing output (down from a peak of 84 percent), and less that 10 percent of the global military manpower (down from 45 percent).[46]

Although discounted by some critics, his assertions are troubling. The advancements of the Information Age revolution, which spurred the rapid growth of global communications, now provide almost any nation with the ability to develop into a regional threat. Joint Vision 2010 notes America's advanced technology provides U.S. forces with many advantages. However, it also warns that we can expect future adversaries will actively and passively exploit technology to improve their military capability and to counter U.S. military strength.[47]

The growth of these global information networks is expanding faster than the military can figure out what or how to defend them. This speed of acceleration is discomforting to military leaders.[48] Slowly the military is recognizing that it is neither completely capable of, nor totally responsible for defending all of these networks. Yet, the military must clearly define its responsibilities for protecting America's vital interests in these global infrastructures. The military must also work to develop new relationships with law enforcement, corporations, and civilian concerns for sharing in the defense of these infrastructures. Certainly it must maintain a core competency in areas such as cryptology, but it must also succeed in reforming its strategic outlook and organizational structure.[49]

CONCLUSION:

The Strategic Principles of War are a useful analytical tool. They provide strategic military planners a useful methodology to examine the complex implications of policy decisions within a framework focused on the defense of America. Many of the initial steps in implementing the leveraging of civilian operations and developing Information Superiority are

already underway. In many cases, the President's Commission on Critical Infrastructure Protection was the springboard to action. It provided the nexus between the government, military, law enforcement and industry to come together in pursuit of a common objective. Viewed in relation to the Strategic Principles of War, leveraging civilian systems for future strategic operations requires addressing the following issues:

1. Objective: Technical and fiscal imperatives require U.S. strategic communications shift from military owned and operated networks to highly leveraged commercial global information grids. Strategic communications will become a subset of these information grids.

The success of such leveraging will rely more on the military's development of Information Superiority than it will on leveraging civilian operations. Leveraging civilian operations can provide the way to strategic communications for the military, but only if Information Superiority provides them the means to succeed.

2. Initiative: Fully leverage all civilian strategic communication undertakings to promote a robust, redundant, reconfigureable network for the transfer of information. Develop

the warriors and the organizations necessary to support them. Fund technology which provides the leading edge tools for network access and control, data-mining, and the processes which focus on the ability create to knowledge.

3. Unity of Effort: Create global partnerships between government, military, private, and commercial entities which will enhance America's efforts to defend her interests and succeed in the global political and economic realms.

4. Focus: Remove the seams which create communication barriers and friction. Elimination of these hindrances between the various elements of government, the military, and law enforcement (as well as with America's commercial partners) will also enhance the decision-making timeline. Create a "national level of trust" by clearly articulating America's objectives toward information assurance and by developing the security procedures which support this goal.

5. Economy of Effort: In certain industrial sectors the concept of the Defense Technology and Industrial Base may need re-examination. Where appropriate, align DTIB with the concept of Commercial-Military Integration.

6. Orchestration: Support national and international efforts for standardization in communication technology.

7. Clarity: Clarify the future roles for the military, as well as for law enforcement and industry, to defend America. Reshape U.S. military forces warfighting structures to accommodate these changes in roles.

8. Surprise: The U.S. should take the lead in promoting assured protection to the global information grids. If and where appropriate, create alliances or treaties to enhance this protection.

9. Security: The linchpin of the Strategic Principles of War and also the key enabler of Information Superiority is security. Certainly security will also be most difficult principle to achieve in the leveraging of civilian operations. And information operations, either offensive or defensive, will require the U.S. to maintain technical leadership in cyrptology, which is the essence of information security.

The policy of leveraging civilian operations for strategic communications has significant implications for the future defense of America. Information and its transmission is significantly changing not only the future ability of people to communicate with each other but also the future of warfare, and even how a nation defines itself. America's best hope for

defending itself in this emerging world of information resides in the concept of Information Superiority, especially the asymmetrical advantages it will provide.

6,557

ENDNOTES

[1] Alvin and Heidi Toffler, "Future Shock and Global Telecommunications," Available from <http://www.iridium.com/public.fall.pubvce.html>; Internet; accessed 12 January 1998.

[2] Steven Lubar, "Considering the Age of Information,"; available from <http://www.iridium.com/public.fall.pubvce.html>; Internet; accessed 12 January 1998.

[3] Defense Information Systems Agency, Master Plan, Available from <http://www.dia.mil:80/DISN/disnar1.html>; Internet; accessed 17 January 1998.

[4] William T. Johnsen, et al., The Principles of War in the 21st Century: Strategic Considerations, Strategic Studies Institute, (U.S. Army War College, Carlisle Barracks: 1 August 1995), 37.

[5] Chairman, Joint Chiefs of Staff, Doctrine for Joint Operations, Joint Pub 3-0, (Washington, D.C.:Joint Staff, 1 February 1995), Appendix A.

[6] Johnsen, 37.

[7] Ibid, 2.

[8] Ibid. 4. For ease of reference, the definitions for each of the nine Principles of War are reprinted here.

[9] President of the United States, A National Security Strategy for a New Century, (Washington, D.C.: U.S. Government, May 1997),5.

[10] "Defense Information Systems Agency (DISA), "Master Plan".

[11] Chairman, Joint Chiefs of Staff, Joint Vision 2010.

[12] "Space Communications Architecture," 29 August 1996; available from <http;//www.acq.osd.mil/space/architectu/space.html>; Internet; accessed 12 January 1998.

[13] Ibid.

[14] Dr. Paul G. Kaminski, "A Year Later: A Report Card - Any Outside the Box Thinking?" Keynote Address to the 2nd Annual Space Policy and Architecture Symposium, 17 February 1997; available from <http://www.acq.osd.mil/space/programs/execsum/center-left.html>; Internet; accessed 12 January 1998.

[15] Johnsen, 6.

[16] Burke, James, Connections (Boston, MA.:Little Brown, 1978).

[17] P.T.Hengst, LTC, USA, "Managing the Intelligent Information Grid for the Army After Next" p. 6

[18] Schwartau, Winn, Information Warfare, (New York:Thunder's Mouth Press, 1994).

[19] National Defense Panel, Report of: "Transforming defense: National Security in the 21st Century", (Arlington, VA: Secretary of Defense, December 1997) 66.

[20] Hengst, 2.

[21] George I. Zyzman, "Wireless Networks", Scientific American, Vol.273, No 3 (September 1995): 71.

[22] Samuel P. Huntingdon, The Clash of Civilizations and the Remaking of World Order, (New York, Simon and Schuster, 1996),67.

[23] Johnsen, 9.

[24] DR Paul G. Kaminski, "A Year Later: A Report Card - Any Outside the Box Thinking?" Keynote Address to the 2nd Annual Space Policy and Architecture Symposium, Washington, D.C. 11 February 1997.

[25] "Iridium Gets U.S. as First Customer of Wirelss Communication System," *Wall Street Journal, 26 January 1998, sec B7, p.1.*

[26] "Fast Facts About Iridium," available from <http://www.iridium.com/gloss/glglnc.html>; Internet; accessed 18 January 1998.

[27] *Wall Street Journal, p.1.*

[28] Headquarters U.S. Space Command, "Global Partnerships Working Draft, U.S. Space Command," (Peterson Air Force Base Colorado, 25 June 1997), GP1-43.

[29] Felix Gilbert, "Machiavelli: The Renaissance of the Art of War," in Makers of Modern Strategy, ed Peter Paret, (Princeton, New Jersey: Princeton University Press, 1986), 18.

[30] Johnsen, 11.

[31] Presidents Commission on Critical Infrastructure Protection (PCCIP), Report on Critical Foundations, Protecting America's Infrastructures, (Washington, D.C., October 1997), 47-59.

[32] Ibid.

[33] Johnsen, 14.

[34] *Boezer, Gordon, Ivars Gutmanis, and Joseph E. Muckerman II, "The Defense Technology and Industrial Base: Key Component of National Power," Parameters, Vol. 28 No 3, Summer 1997, 46.*

[35] Ibid, 26.

[36] Ibid, 39.

[37] Johnsen, 15.

[38] Johnsen, 18.

[39] Johnsen, 20.

[40] John Arquilla, "The Great Cyberwar of 2002", Wired, 6.02, February 1998, 122.

[41] Department of the Army, The Army Satellite Communications (SATCOM) Architecture, (Fort Gordon, GA: U.S. Army Training and Doctrine Command, April 1970), 9-3.

[42] Ibid. 9-4.

[43] Johnsen, 22.

[44] Defense Science Board (DSB)Task Force, "Report on Information Warfare - Defense (IW-D)," Secretary of Defense (Washington, D.C.: November 1996), Available by Interpact, Inc. at www.infowar.com>; Internet. Accessed 10 October 1997. ES-1.

[45] Huntingdon, 88.

[46] Ibid, 91.

[47] Chairman, Joint Chiefs of Staff, Concept for Future Joint Operations, Expanding Joint Vision 2010, (Washington, D.C.:Joint Staff, May 1997),14.

[48] Alvin and Heidi Toffler, "Future Shock and Global Telecommunications," available from <http://www.iridiiium.com/public/summer/pubvce.html>; Internet; accessed on 12 January 1998.

[49] President's Commission on Critical Infrastructure Protection, The Report on the Critical Foundations, Protecting America's Infrastructure (Washington, D.C.:Presidents Commission on Critical Infrastructure Protection, October 1997),50.

BIBLIOGRAPHY

Adelman, Kenneth L. and Norman R. Augustine, The Defense Revolution, Strategy for the Brave New World. San Francisco: Institute for Contemporary Studies Press, 1990.

Alberts, David S. and Daniel S Papp. Information Age Anthology. Washington D.C., National Defense University. June 1997.

Bernstein, Alvin H., Martin Libicki and Frederick W. Kagan. "High-Tech: The Future Face of War?." Commentary. January 1998, 29-34.

Boezer, Gordon, Ivars Gutmanis, and Joseph E. Muckerman II. "The Defense Technology and Industrial Base: Key Component of National Power" Parameters Vol. 28 No 3 (Summer 1997), 26.

Burke, James. "Connections." Boston: Little Brown. 1978.

Chairman, Joint Chiefs of Staff, Joint Vision 2010. Washington, D.C.:Joint Staff. 1997.

Chairman, Joint Chiefs of Staff, Concept for Future Joint Operations, Expanding Joint Vision 2010. Washington, D.C.:Joint Staff. May 1997.

Chairman, Joint Chiefs of Staff, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington, D.C.:Joint Staff. 4 July 1996.

Chairman, Joint Chiefs of Staff, Joint Warfare of the Armed Forces of the United States. Joint Pub 1. Washington, D.C.:Joint Staff. 10 January 1995.

Chairman, Joint Chiefs of Staff, Doctrine for Joint Operations. Joint Pub 3.0. Washington, D.C.:Joint Staff. 1 February 1995.

Defense Information Systems Agency. Master Plan. Available from <http://www.dia.mil:80/DISN/disnar1.html>. Internet. Accessed 17 January 1998.

Defense Science Board (DSB). Report on Information Warfare-Defense (IW-D). Office of the Under Secretary of Defense for Acquisition and Technology. Washington, D.C.:November 1996.

Available from Interpact, Inc. at <www.infowar.com>. Internet. Accessed 10 October 1997.

Department of the Army. The 1997 Army Satellite Communications Architecture Book. Fort Gordon, GA: U.S. Army Training and Doctrine Command. Published by Information Technology and Applications Corporation. Reston, VA. April 1997.

Dunnigan, James F. Digital Soldiers, The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield. New York: St Martins's Press. 1996.

"Exercise Demonstrates Benefits of Military's Network-Centric Warfare." Signal. November 1997.

"Fast Facts About Iridium." Available from <http://www.iridium.com/gloss/glglnc.html>; Internet. Accessed 18 January 1998.

"Future War: Information Operations Corps Comes of Age" Army Magazine. December 1997.

Gilbert, Felix. Machiavelli: The Renaissance of the Art of War." in Makers of Modern Strategy, ed. Paret, Peter. 18. Princeton, New Jersey: Princeton University Press, 1986.

Hardy, Quentein. "Iridium Gets U.S. as First customer of Wireless Communication System." Wall Street Journal, 26 January 1998, sec B7, p.1.

Headquarters U.S. Space Command. "Global Partnerships, Working Draft." U.S. Space Command Long Range Plans. Peterson Air Force Base, Colorado. 26 June 1997. GP1-43.

Hengst, P.T., LTC, USA. Managing the Intelligent Information Grid for the Army After Next. USAWC Military Studies Program Paper. U.S. Army War College, Carlisle Barracks, PA 17013. 1 April 1997.

Huntingdon, Samuel P. The Clash of Civilizations and the Remaking of the World Order. New York:Simon and Schuester. 1996.

Johnson, Robert E., LTC (P), USA Information Warfare: Impacts on Command and Control Decision Making. USAWC Military Studies Program Paper, U.S. Army War College, Carlisle Barracks, PA 17013. 15 April 1996.

Johnsen, William T., Douglas V. Johnson, James O. Kievit, Douglas C. Lovelace Jr, and Steven Metz. The Principles of War in the 21st Century: Strategic Considerations. Strategic Studies Institute. U.S. Army War College. 1 August 1995.

Josephson, Edward H. and Raymond M. Macedonia. Fighting Smarter: Leveraging Information Age Technology. The Institute of Land Warfare. Association of the United States Army. August 1994.

Kaminski, Paul G. Dr., "A Year Later: A Report Card - Any Outside the Box Thinking?" Keynote Address to the 2nd Annual Space Policy and Architecture Symposium, February 11, 1997. Available from <http://www.acq.osd.mil/space/programs/execsum/center-left.html>. Internet. Accessed 12 January 1998.

Lubar, Steven. "Considering the Age of Information," Available from <http://www.iridium.com/public.fall.pubvce.html>. Internet. Accessed 12 January 1998.

National Defense Panel, Report of. Transforming Defense: National Security in the 21st Century. Arlington VA.: Office of the Secretary of Defense, December 1997.

National Imagery and Mapping Agency. Geospatial Information Infrastructure Master Plan. Fairfax, Virginia.: National Imagery and Mapping Agency, 1 October 1997.

Negroponte, Nicholas. Being Digital. New York: Alfred A. Knopf,1995.

Negroponte, Nicholas. "Communicating Bits of Information." Available from http://www.iridiuim.com/public/winter/pubvce.html>. Internet. Accessed 12 January 1998.

Nicholson, Tom M. Jr., LTC, USA, "Civil Reserve Information Services (CRIS) Concepts and One Possible Solution", USAWC Military Studies Program Paper, U.S. Army War College, Carlisle Barracks, PA 17013.

Office of the Assistant Secretary of Defense. C4I Handbook for Integrated Planning (CHIP). Washington, DC: C4I Integration Support Activity (CISA), 21 March 1996.

Open Source Solutions. Open Source Intelligence: Professional Handbook 1.1. Oakton, Virginia 15 September 1996.

Office of the President. A National Security Strategy for a New Century. Washington, D.C.: White House. May 1997

President's Commission on Critical Infrastructure Protection. Report on Critical Foundations, Protecting America's Infrastructures. Washington, D.C.: White House. October 1997.

President of the United States. A National Security Strategy for a New Century. Washington, D.C.: White House. May 1997.

Rawlins Gregory J.E. Moths to the Flame. The Seductions of Computer Technology. Cambridge: The MIT Press, XXDATEXX.

Schwartau, Winn, Information Warfare. New York:Thunder's Mouth Press. 1994.

"Space Communications Architecture." 29 August 1996. Available from <http;//www.acq.osd.mil/space/architectu/space.html>; Internet. Accessed 12 January 1998.

Sumser, Raymond J. and Charles W. Hemingway. "The Emerging Importance of Civilian and Contractor Employees to Army Operations." Landpower Essay Series. AUSA Institute of Land Warfare. No 95-4, June 1995.

"The Great CyberWar of 2002", Arquilla, John. Wired. February 1998.

Toffler, Alvin and Heidi. "XXXXXXXXXXXX"; Available from <http://www.iridium.com/public.fall.pubvce.html>. Internet. Accessed 12 January 1998.

Zyzman, George I., "Wireless Networks", Scientific American, Vol.273, No 3, September 1995.